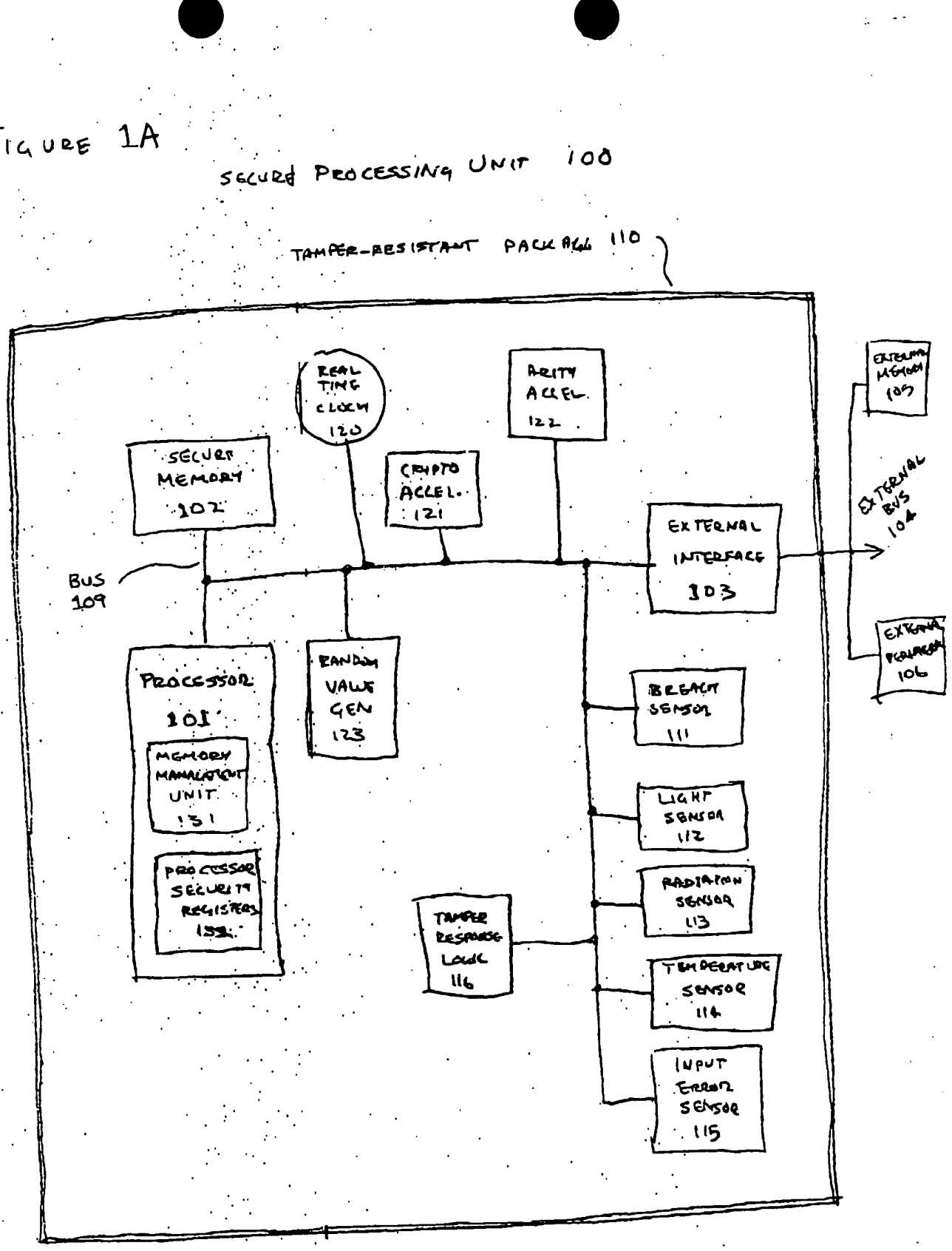
FIGURE 1A


SECURE PROCESSING UNIT 100
TAMPER-RESISTANT PACKAGE 110
REAL TIME CLOCK 120
ARITH ACCEL. 122
SECURE MEMORY 107
CRYPTO ACCEL. 121
EXTERNAL INTERFACE 103
EXTERNAL MEMORY 105
EXTERNAL BUS 104
BUS 109
PROCESSOR 101
MEMORY MANAGEMENT UNIT 131
PROCESSOR SECURITY REGISTERS 133
RANDOM VALUE GEN 123
EXTERNAL PROCESSOR 106
BREACH SENSOR 111
LIGHT SENSOR 112
RADIATION SENSOR 113
TEMPERATURE SENSOR 114
INPUT ERROR SENSOR 115
TAMPER RESPONSE LOGIC 116

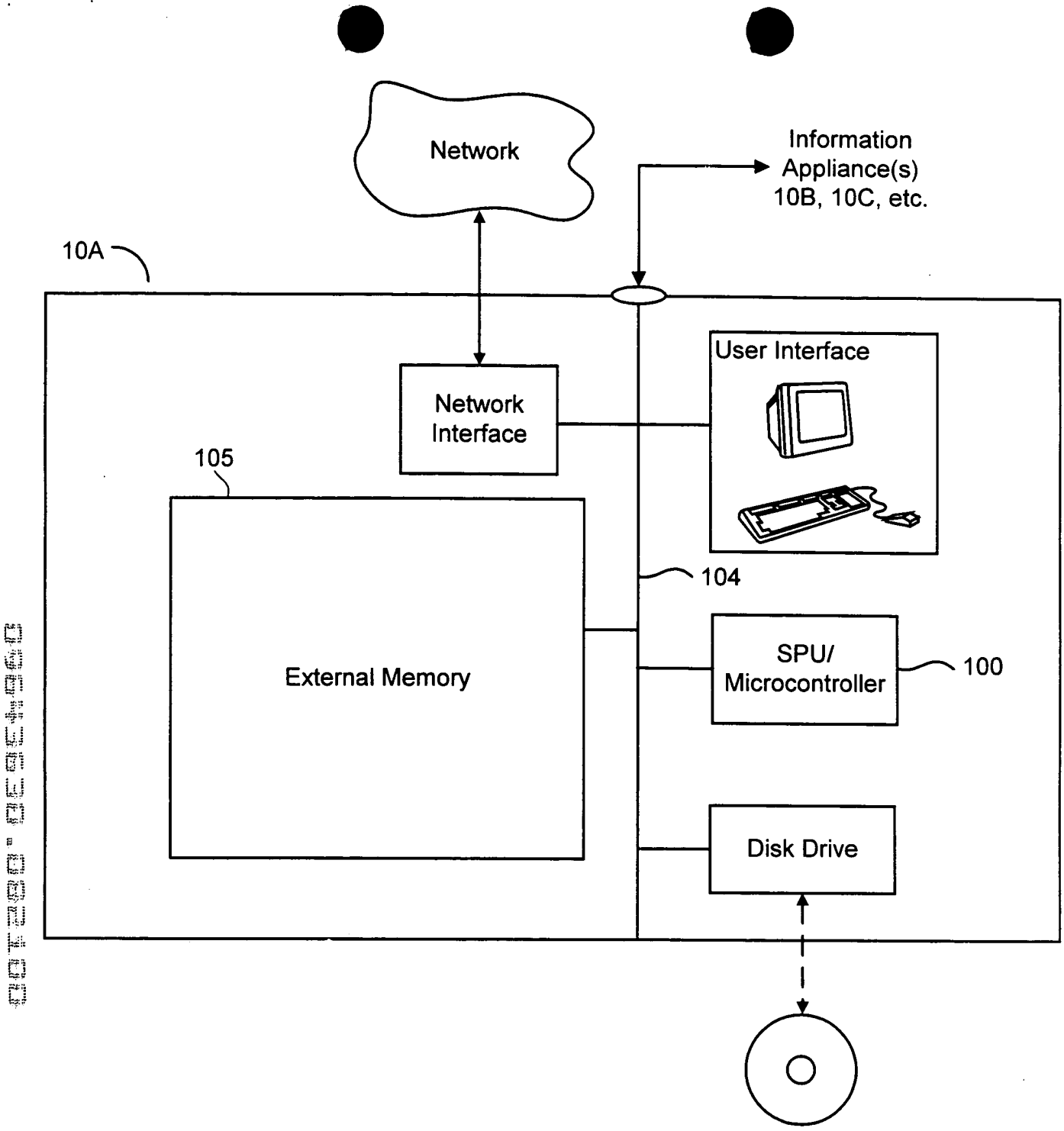

Network
Information Appliance(s) 10B, 10C, etc.
10A
User Interface
Network Interface
105
External Memory
104
SPU/ Microcontroller
100
Disk Drive

Fig. 1B

FIGURE 2

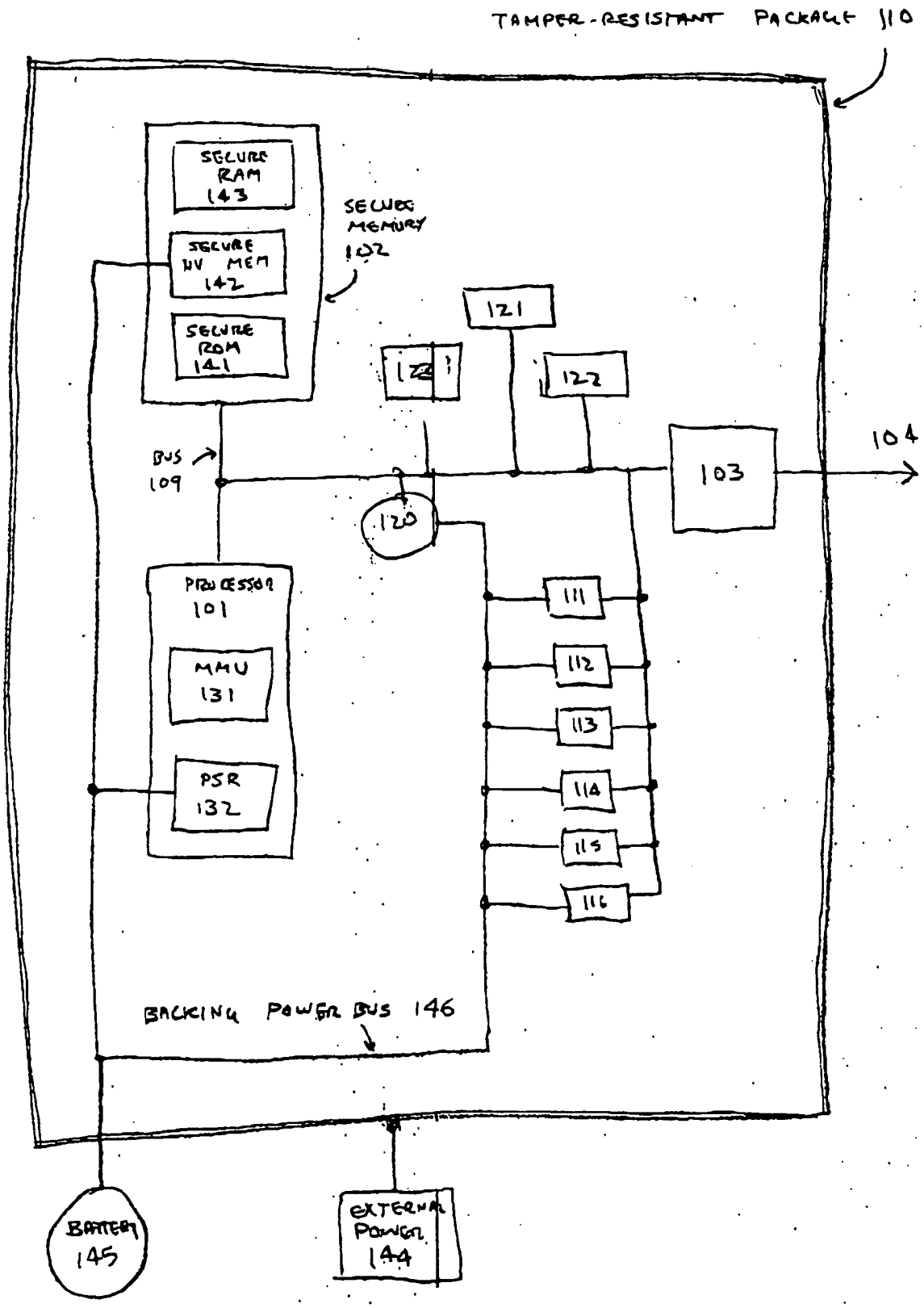

TAMPER-RESISTANT PACKAGE 110
SECURE RAM 143
SECURE NV MEM 142
SECURE ROM 141
SECURE MEMORY 102
121
122
BUS 109
103
104
120
PROCESSOR 101
MMU 131
PSR 132
111
112
113
114
115
116
BACKING POWER BUS 146
BATTERY 145
EXTERNAL POWER 144

FIGURE 3

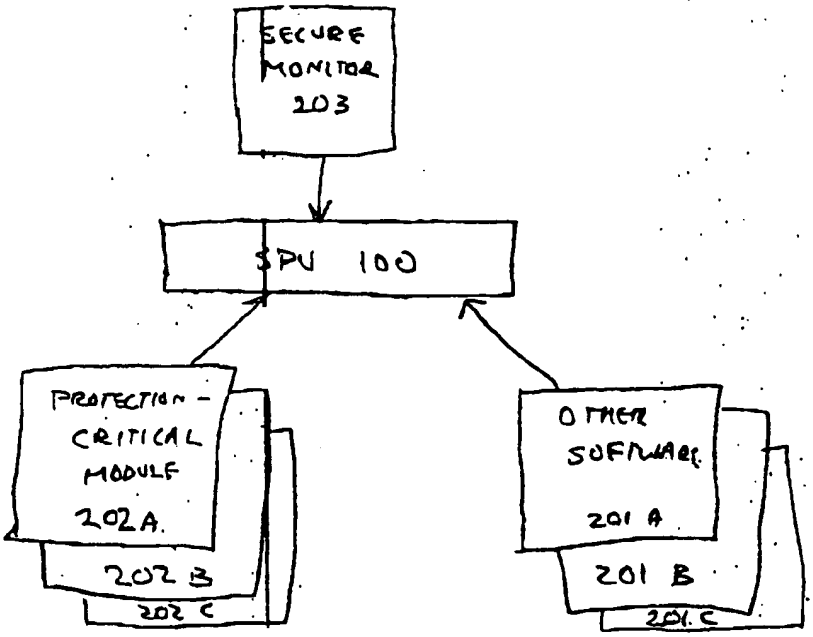
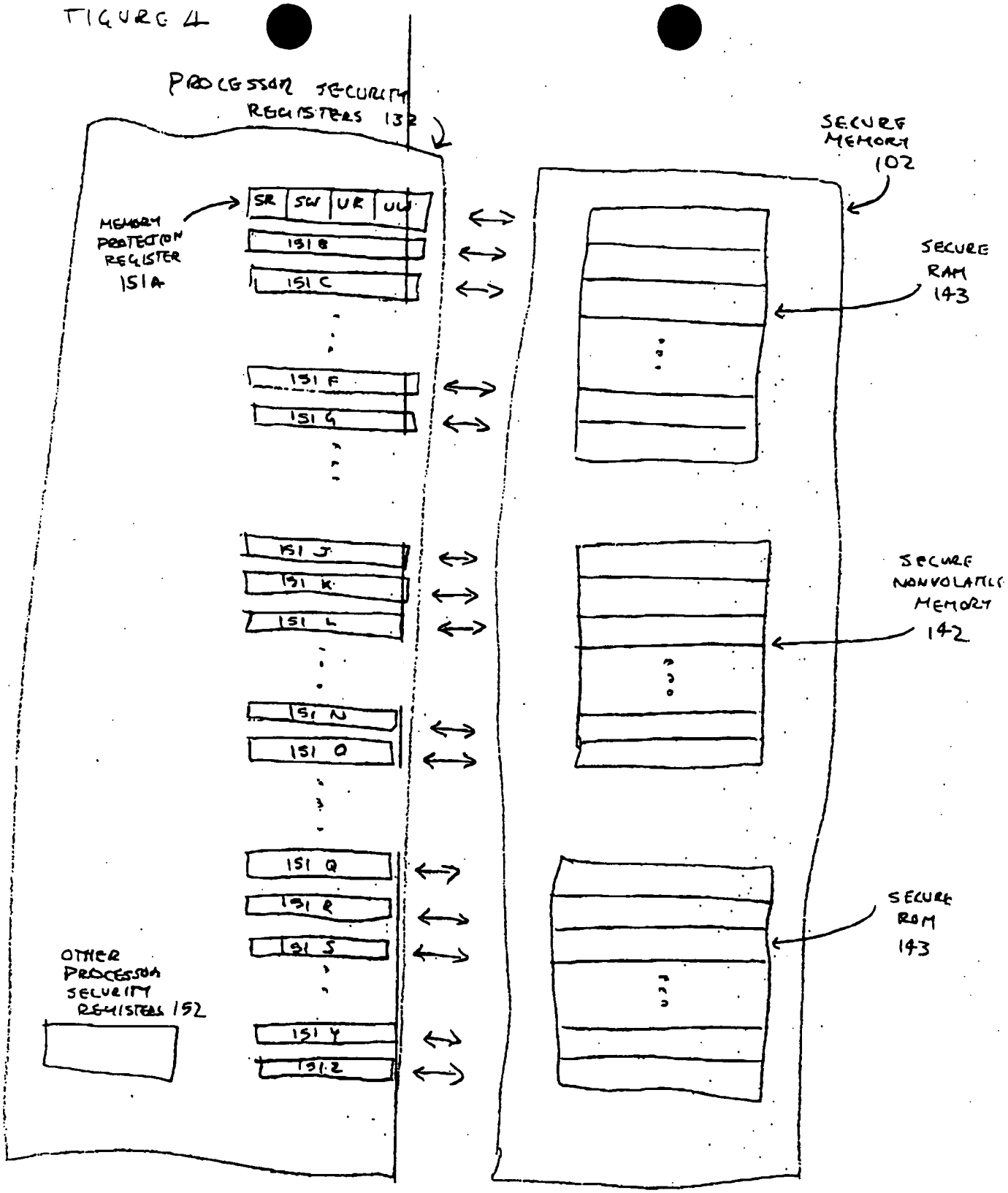

SECURE MONITOR 203
SPU 100
PROTECTION - CRITICAL MODULE 202A
202 B
202 C
OTHER SOFTWARE 201 A
201 B
201 C

FIGURE 4



Attorney Docket No.

FIGURE 5

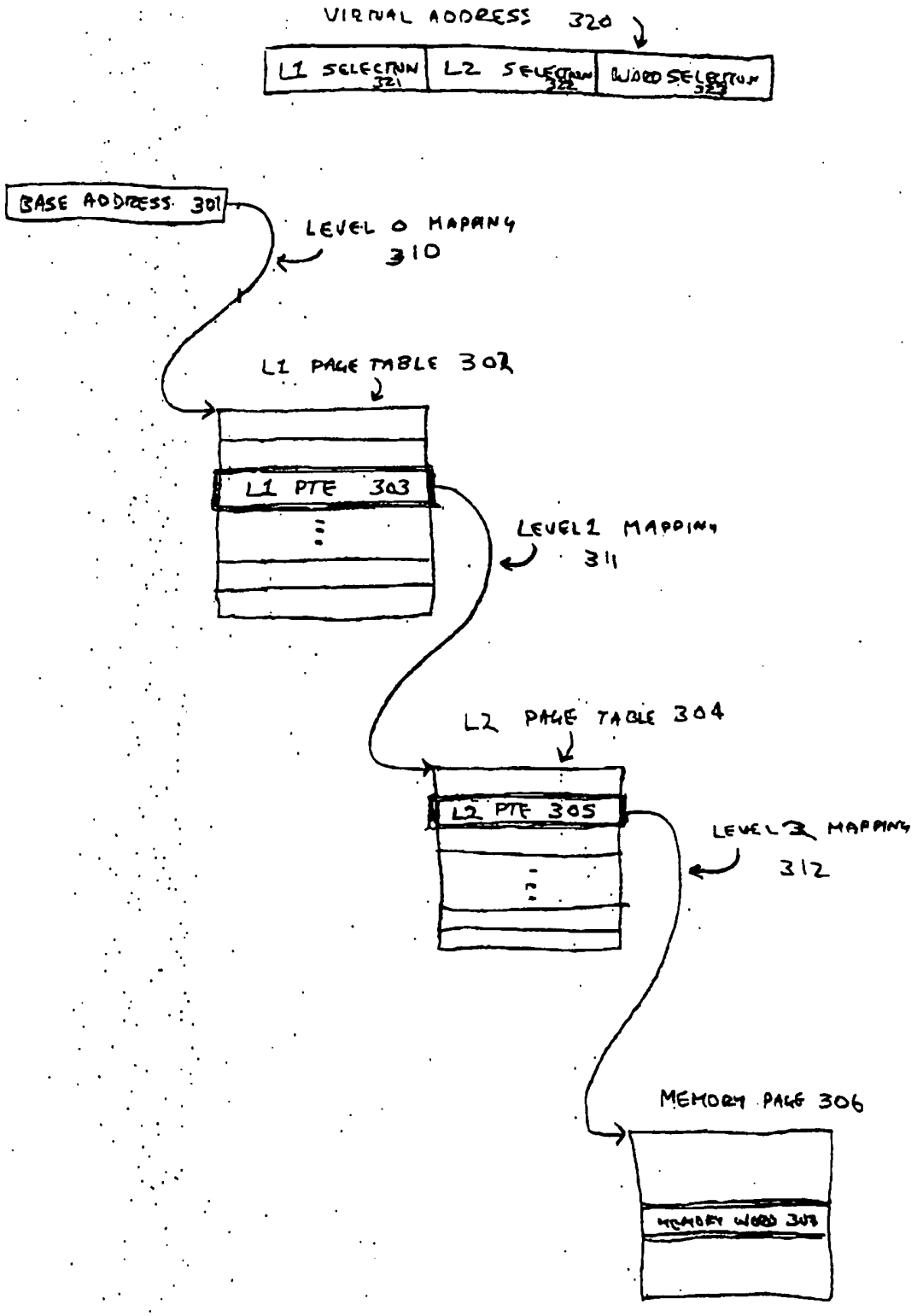
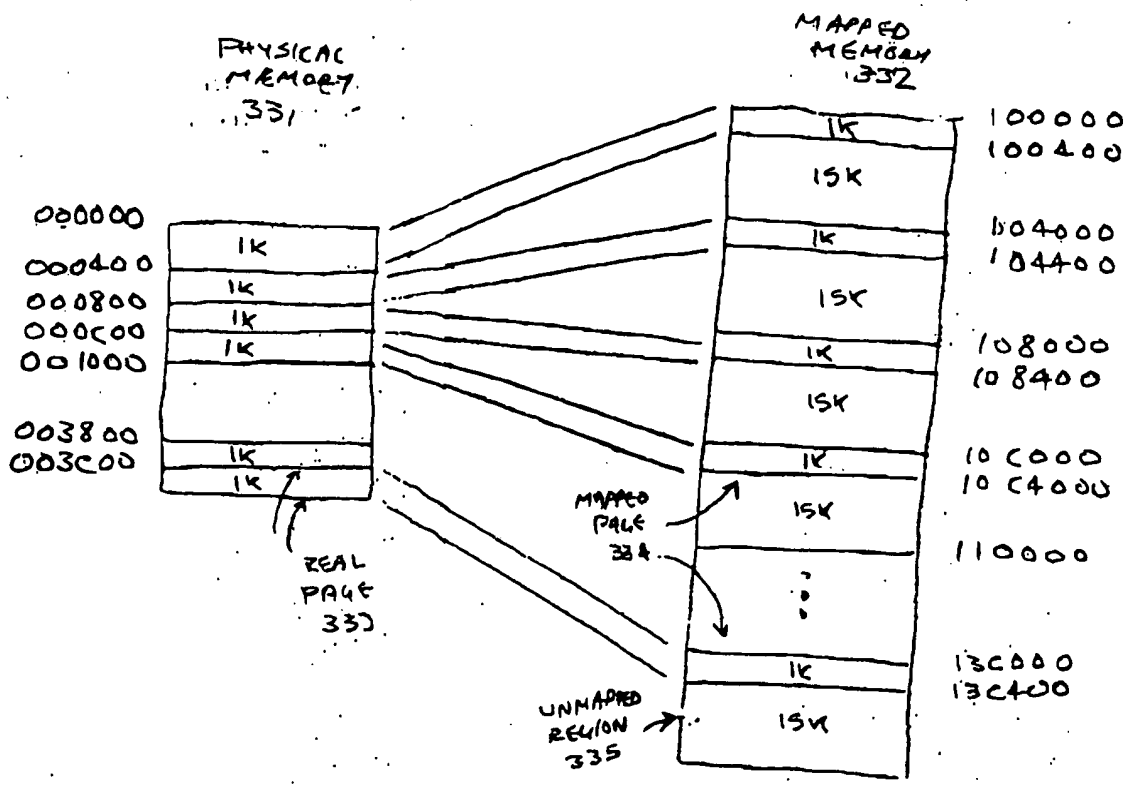

VIRTUAL ADDRESS 320
L1 SELECTION 321
L2 SELECTION 322
WORD SELECTION 323
BASE ADDRESS 301
LEVEL 0 MAPPING 310
L1 PAGE TABLE 302
L1 PTE 303
LEVEL 1 MAPPING 311
L2 PAGE TABLE 304
L2 PTE 305
LEVEL 2 MAPPING 312
MEMORY PAGE 306
MEMORY WORD 307

FIGURE 6



DOT2003: 0050450

FIGURE 7

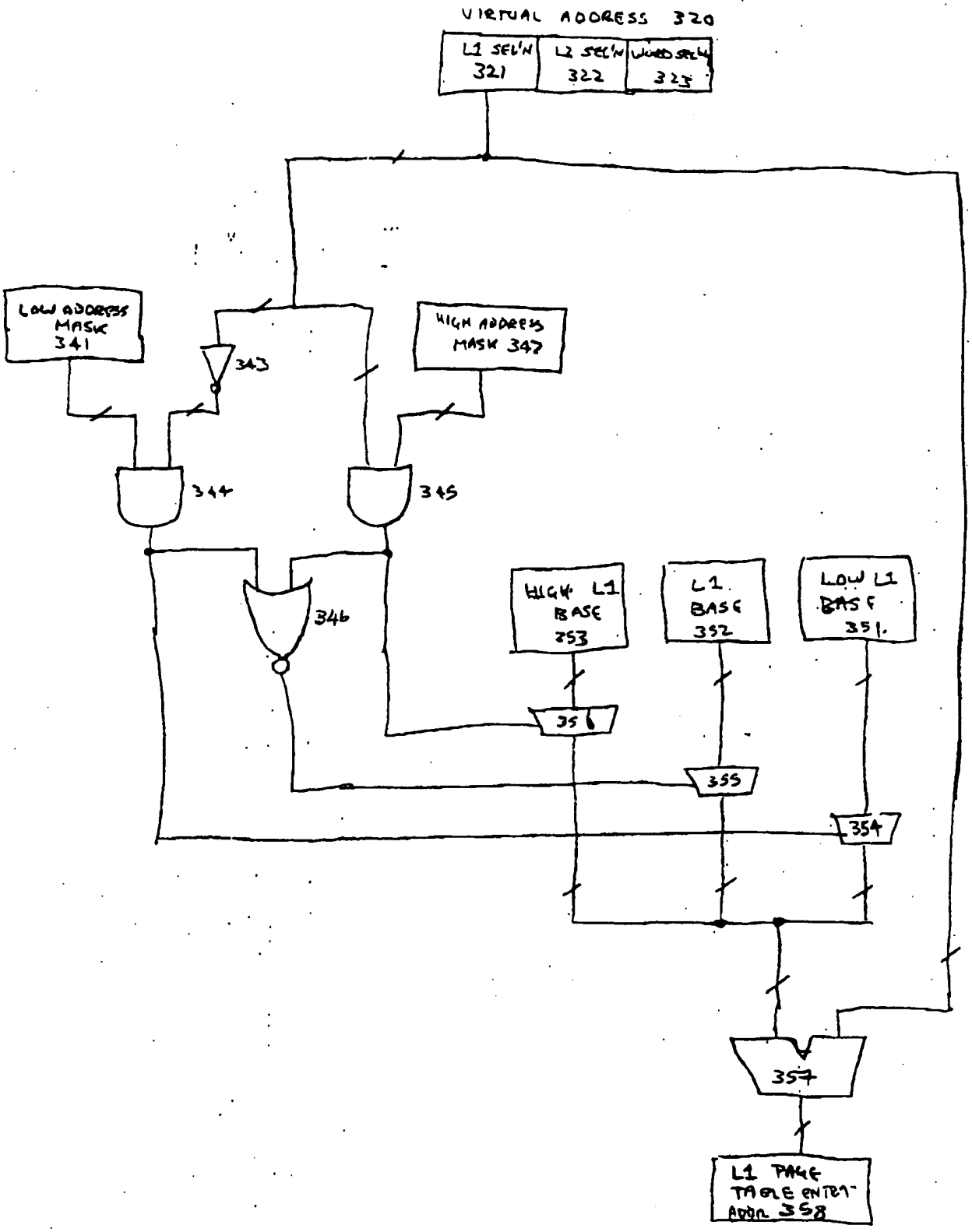

VIRTUAL ADDRESS 320
L1 SEL'N 321
L2 SEL'N 322
WORD SEL'N 323
LOW ADDRESS MASK 341
343
HIGH ADDRESS MASK 347
344
345
346
HIGH L1 BASE 353
L1 BASE 352
LOW L1 BASE 351
356
355
354
357
L1 PAGE TABLE ENTRY ADDR 358

FIGURE 8

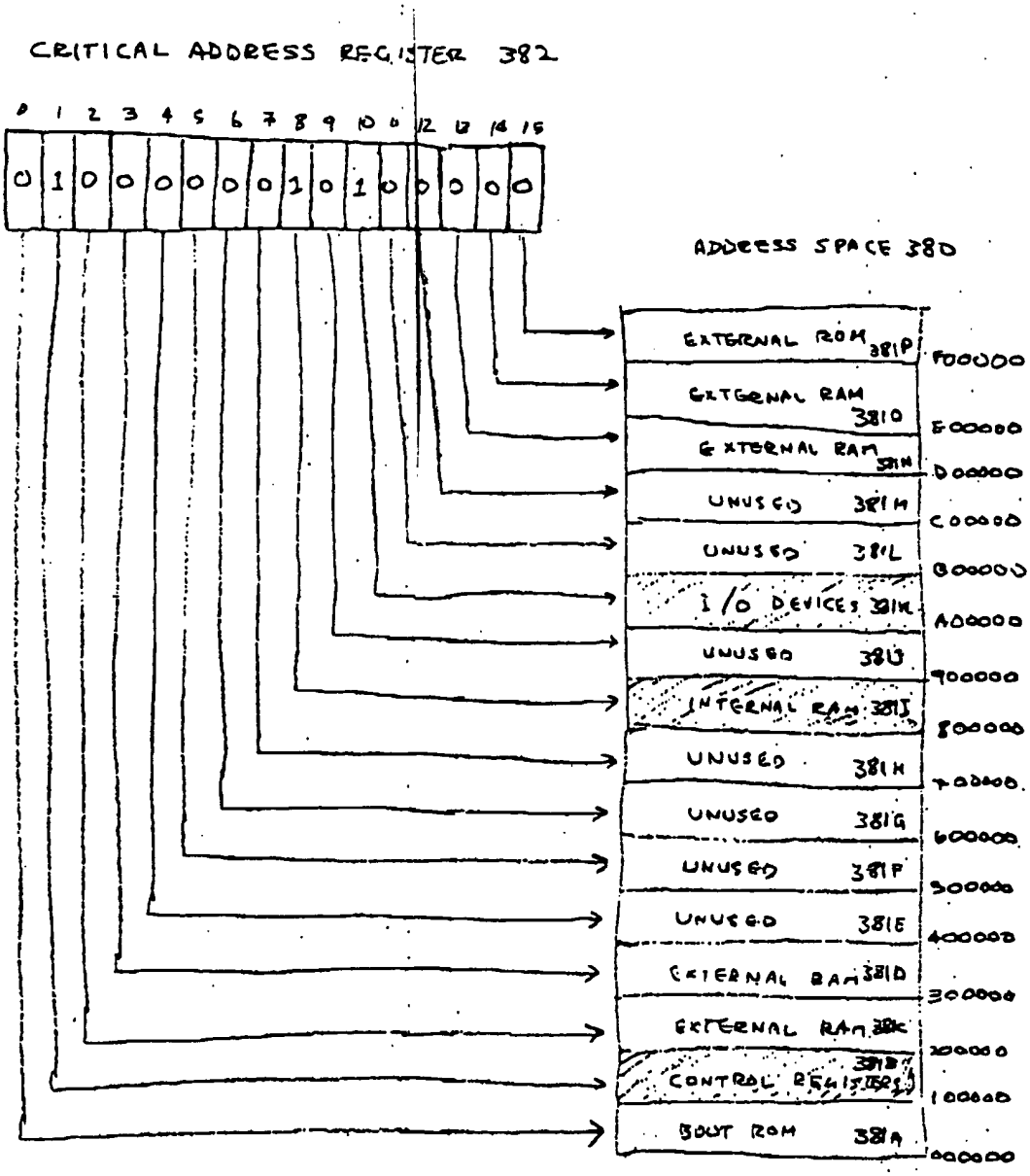

CRITICAL ADDRESS REGISTER 382
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 1 0 0 0 0 0 0 1 0 1 0 0 0 0 0
ADDRESS SPACE 380
EXTERNAL ROM 381P
EXTERNAL RAM 381O
EXTERNAL RAM 381N
UNUSED 381M
UNUSED 381L
I/O DEVICES 381K
UNUSED 381J
INTERNAL RAM 381I
UNUSED 381H
UNUSED 381G
UNUSED 381F
UNUSED 381E
EXTERNAL RAM 381D
EXTERNAL RAM 381C
CONTROL REGISTERS 381B
BOOT ROM 381A
F00000
E00000
D00000
C00000
B00000
A00000
900000
800000
700000
600000
500000
400000
300000
200000
100000
000000

FIGURE 9

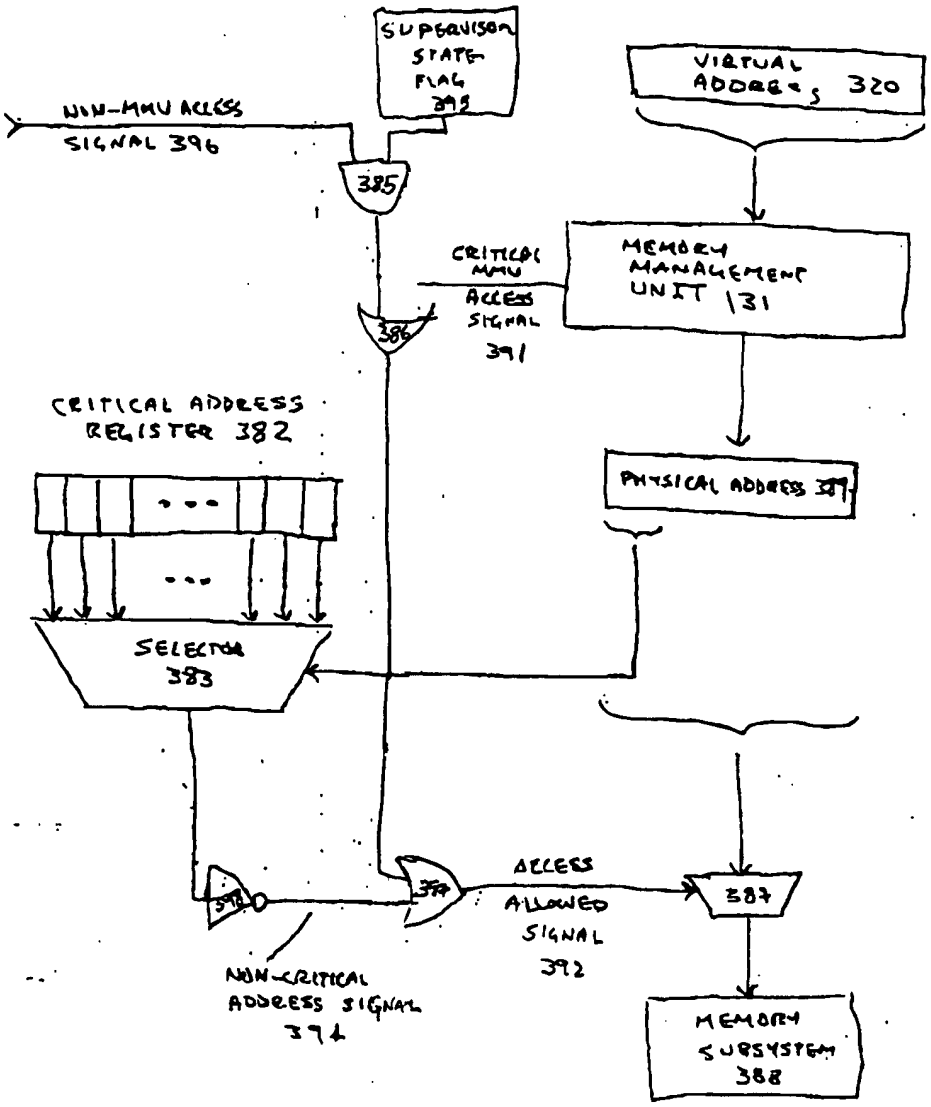

SUPERVISOR STATE FLAG 395
NON-MMU ACCESS SIGNAL 396
385
VIRTUAL ADDRESS 320
MEMORY MANAGEMENT UNIT 131
CRITICAL MMU ACCESS SIGNAL 391
386
CRITICAL ADDRESS REGISTER 382
PHYSICAL ADDRESS 397
SELECTOR 383
378
374
ACCESS ALLOWED SIGNAL 392
387
NON-CRITICAL ADDRESS SIGNAL 394
MEMORY SUBSYSTEM 388

FIGURE 10

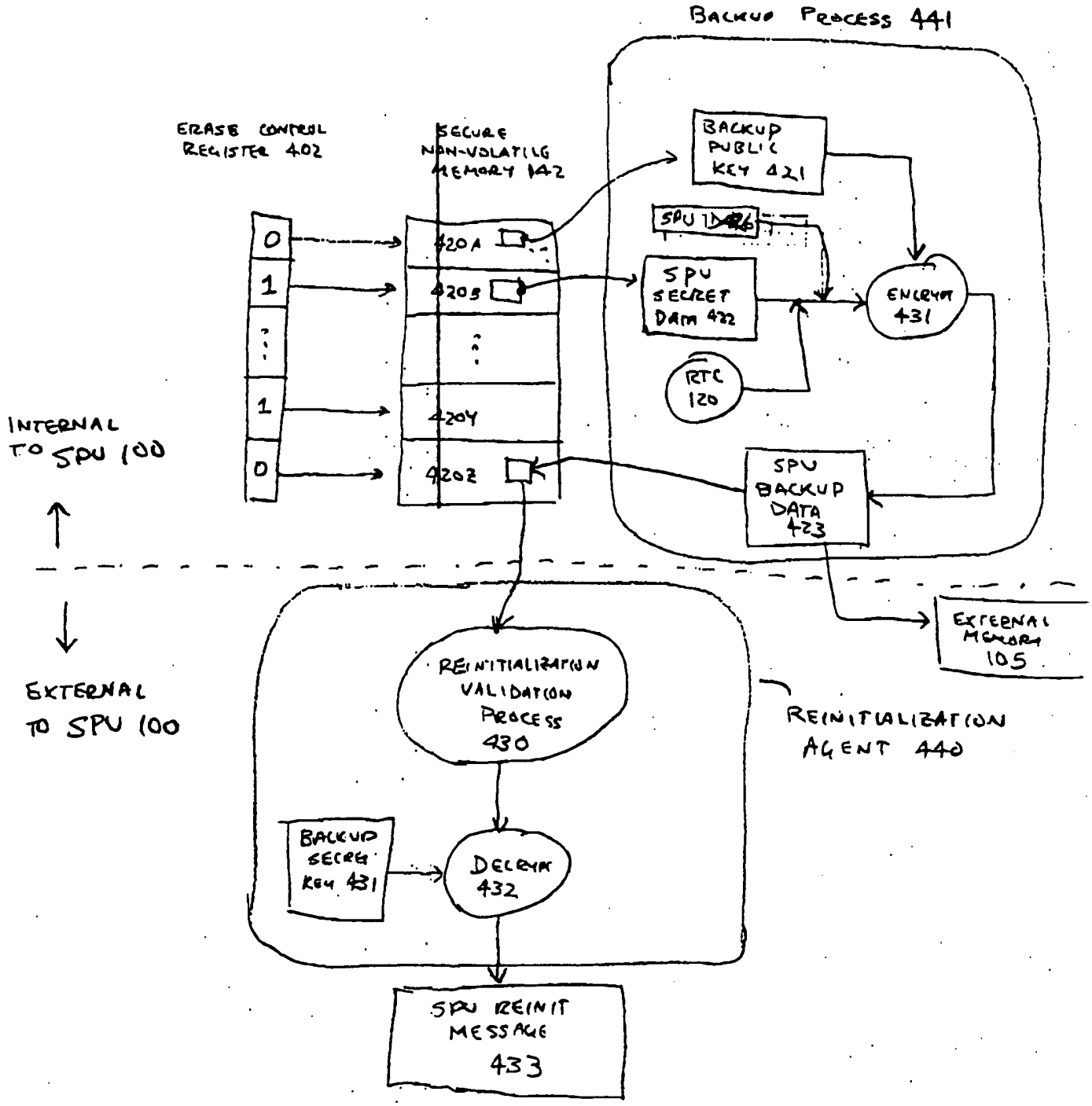

BACKUP PROCESS 441
ERASE CONTROL REGISTER 402
SECURE NON-VOLATILE MEMORY 142
BACKUP PUBLIC KEY 421
SPU ID 426
SPU SECRET DATA 422
ENCRYPT 431
RTC 120
SPU BACKUP DATA 423
0
1
1
0
420A
420B
420Y
420Z
INTERNAL TO SPU 100
EXTERNAL TO SPU 100
EXTERNAL MEMORY 105
REINITIALIZATION VALIDATION PROCESS 430
REINITIALIZATION AGENT 440
BACKUP SECRET KEY 431
DECRYPT 432
SPU REINIT MESSAGE 433

FIGURE 11

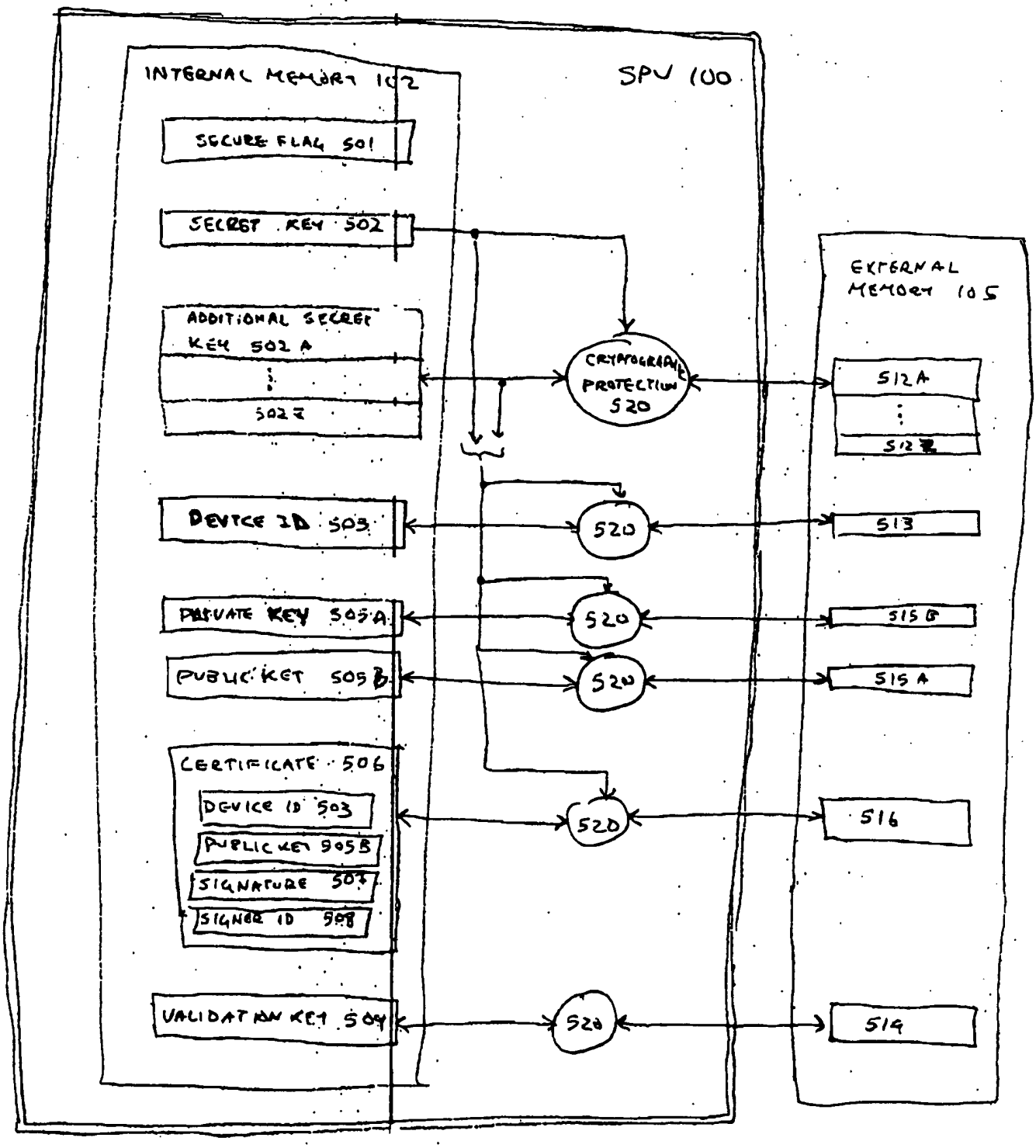
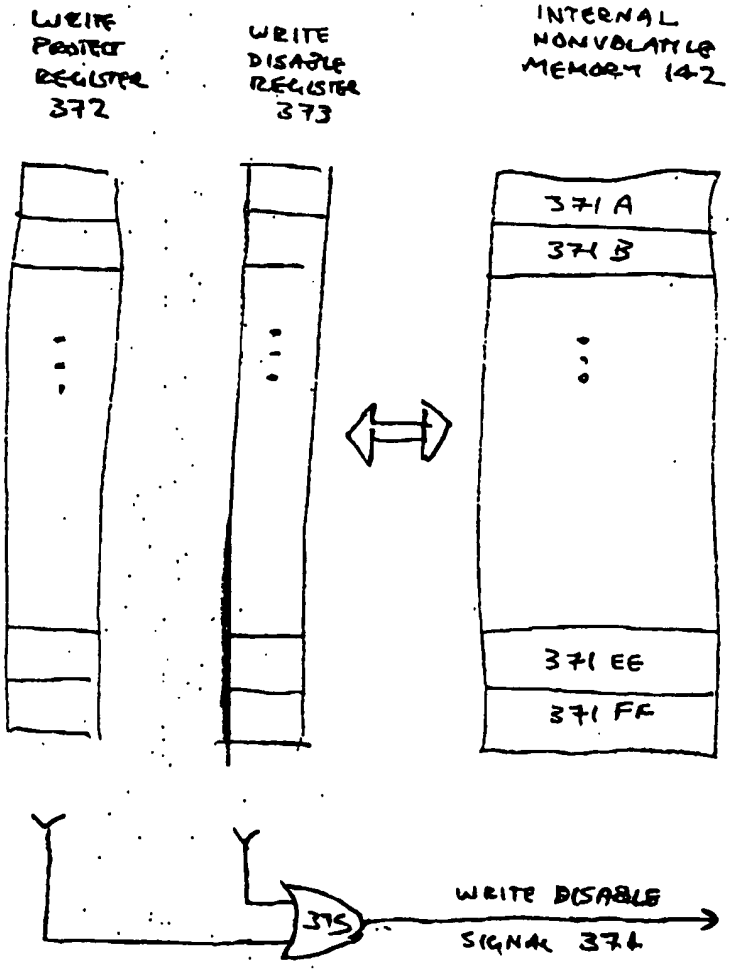

INTERNAL MEMORY 102
SPU 100
SECURE FLAG 501
SECRET KEY 502
ADDITIONAL SECRET KEY 502A
502Z
DEVICE ID 503
PRIVATE KEY 505A
PUBLIC KEY 505B
CERTIFICATE 506
DEVICE ID 503
PUBLIC KEY 505B
SIGNATURE 507
SIGNER ID 508
VALIDATION KEY 509
CRYPTOGRAPHIC PROTECTION 520
520
520
520
520
520
EXTERNAL MEMORY 105
512A
512Z
513
515B
515A
516
519

FIGURE 12



0074280 0C8C4D8

FIGURE 13 — PROTECTED ROM PARTITIONING

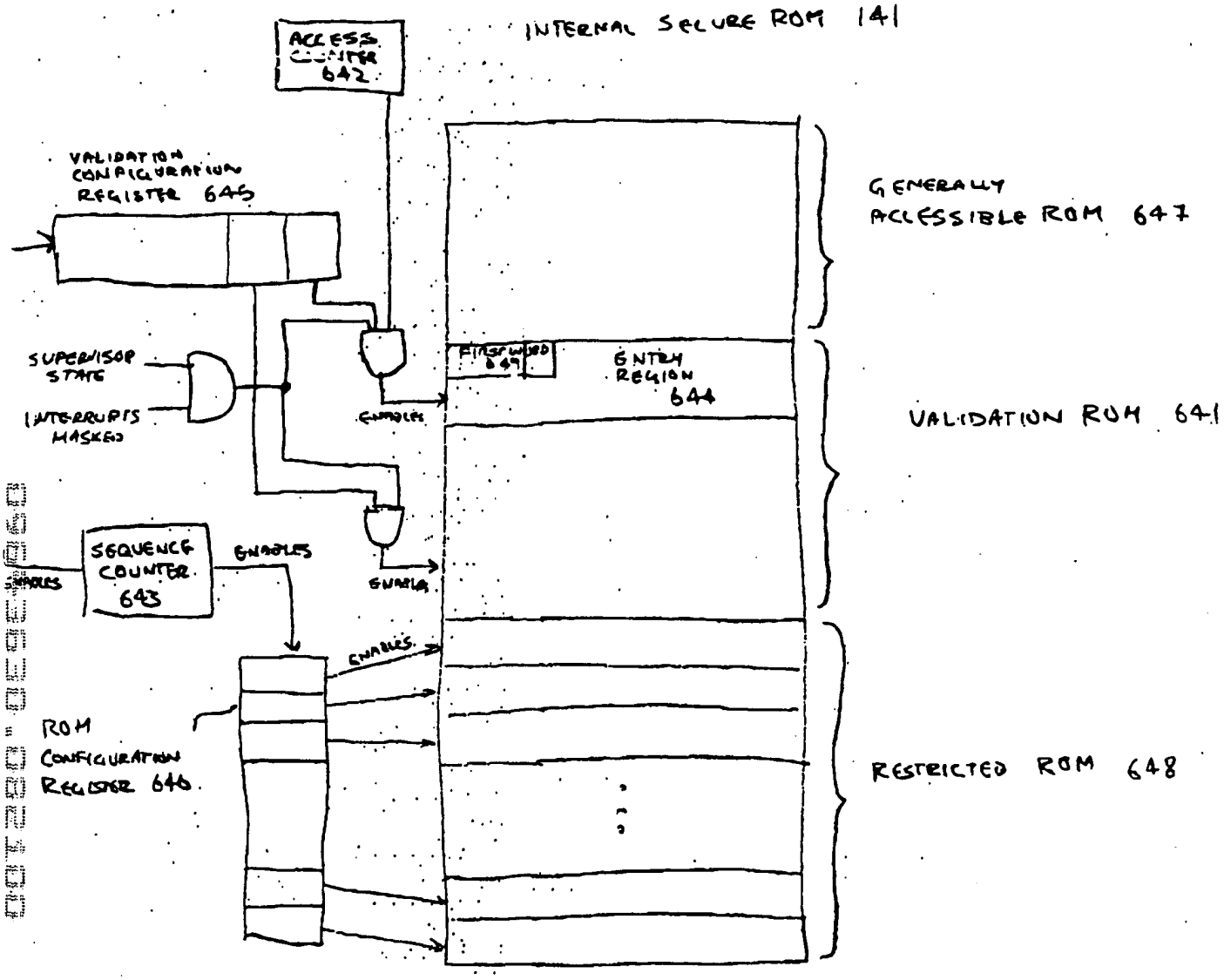


FIGURE 14 – AUTHORIZATION PROOF COMPONENTS

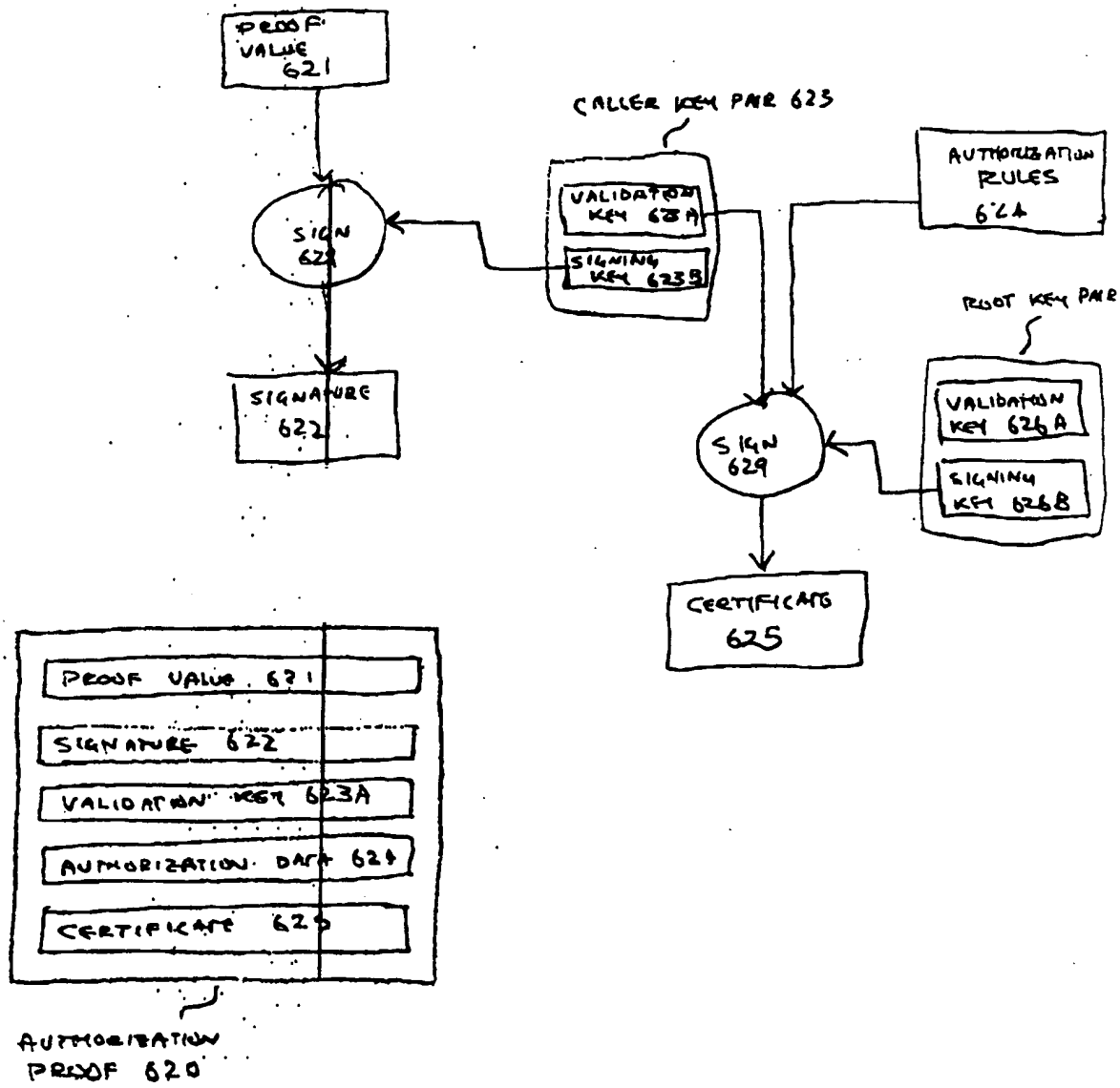


FIGURE 15 -- VALIDATION OPERATION

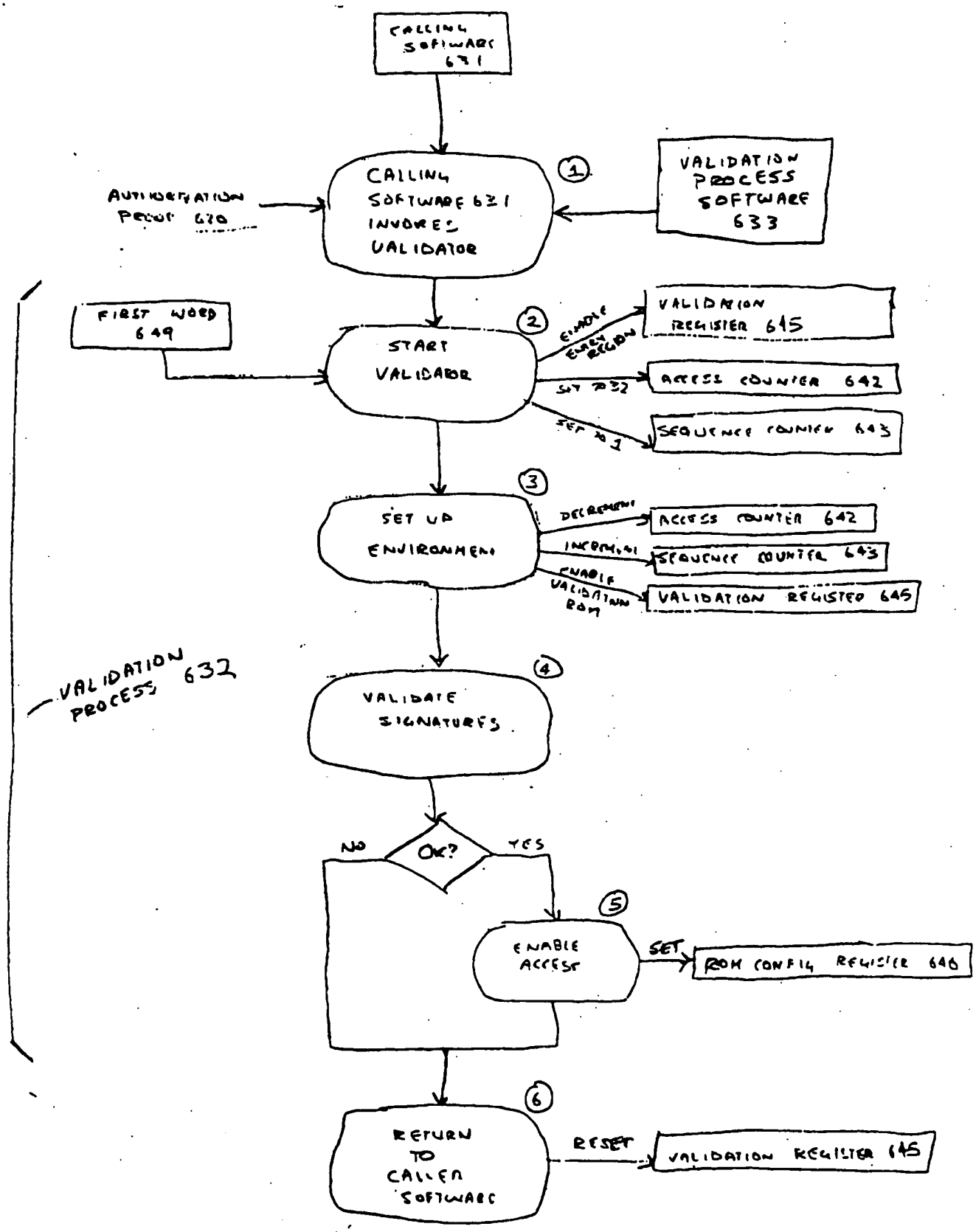


FIGURE 16 – MONITOR SOFTWARE LOAD PROCESS (1)

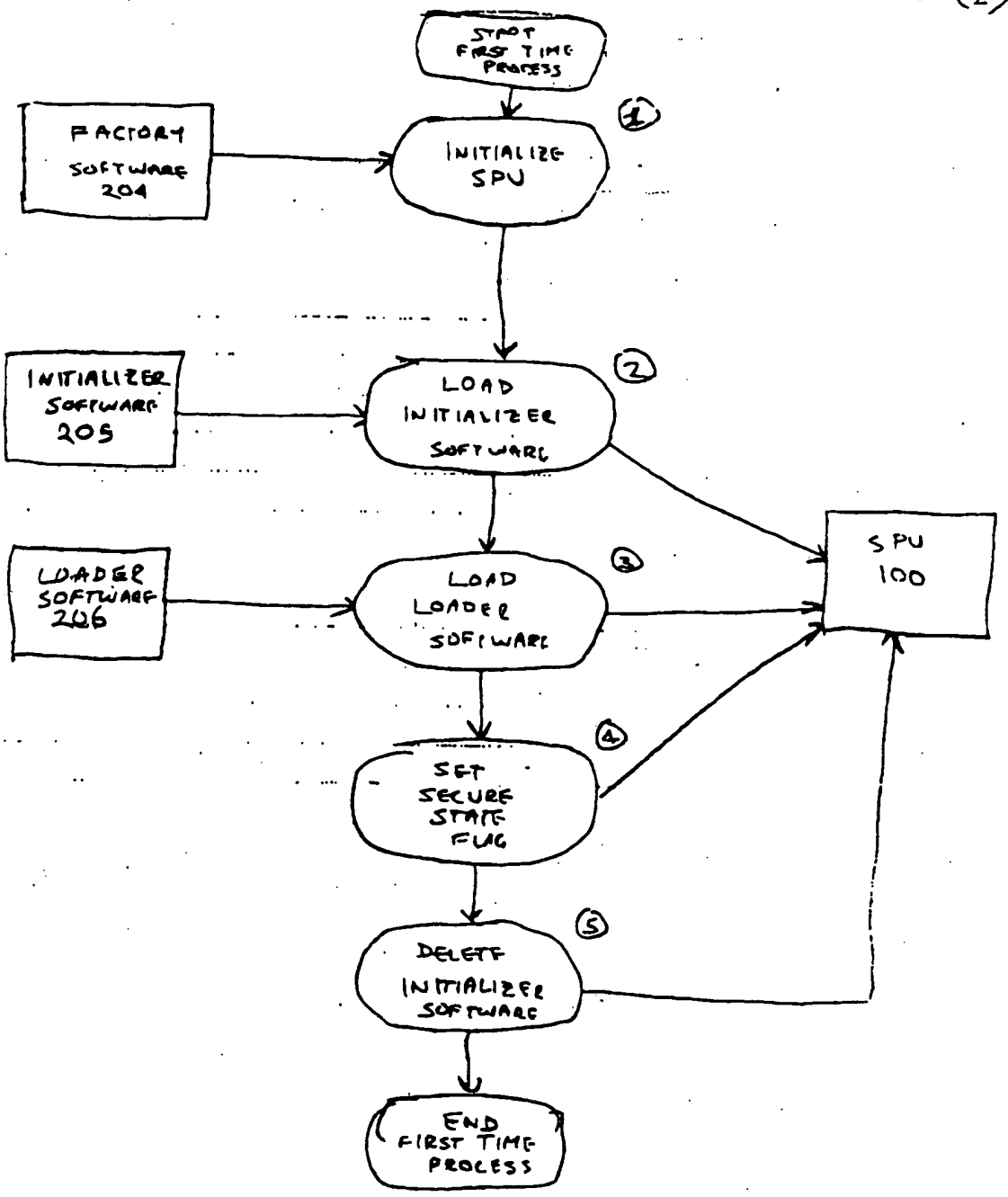


FIGURE 17 - MONITOR SOFTWARE LOAD PROCESS (2)

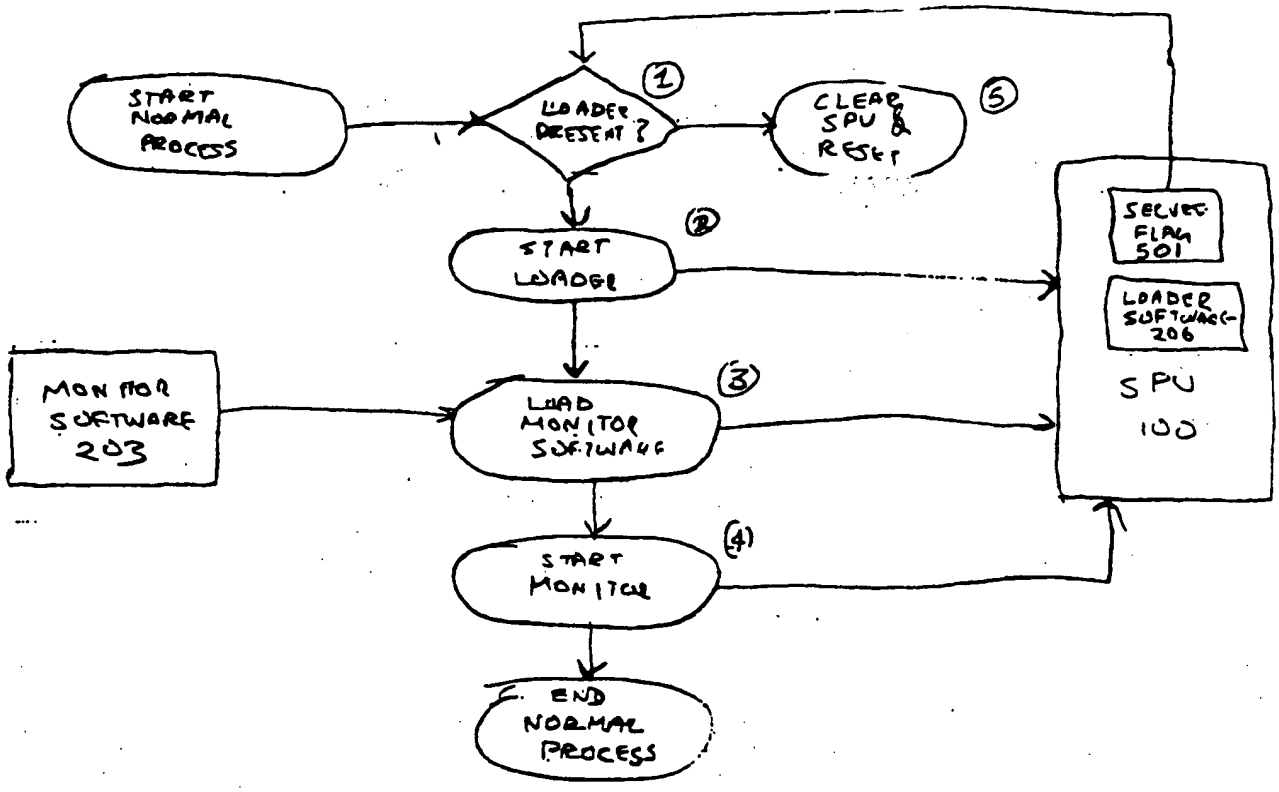
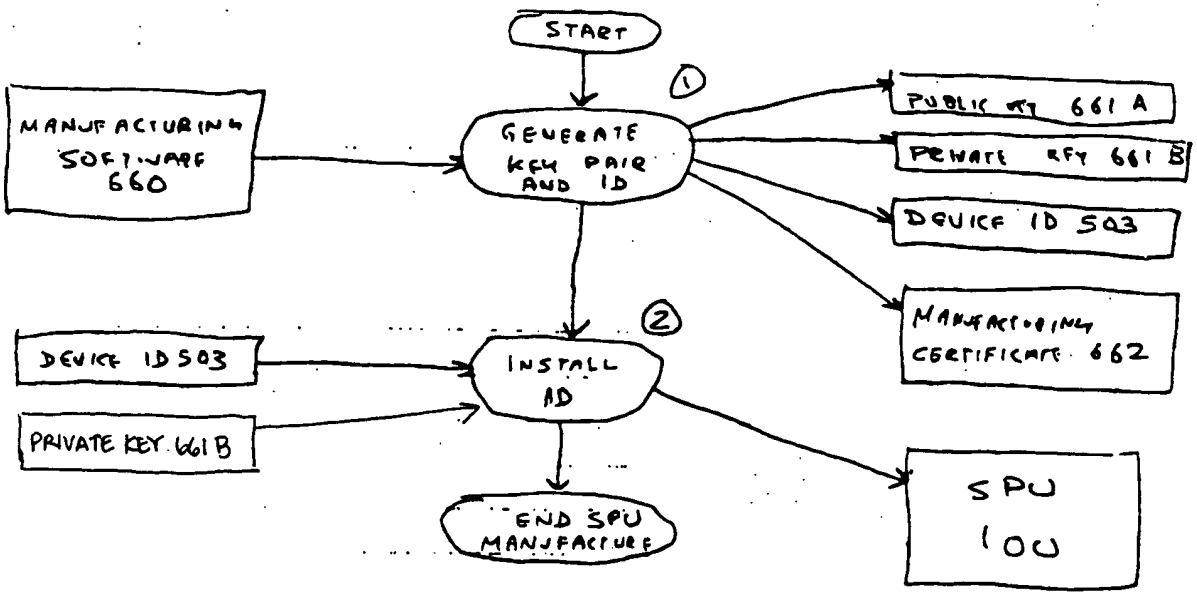


FIGURE 18-A ALTERNATIVE LOAD PROCESS (1)



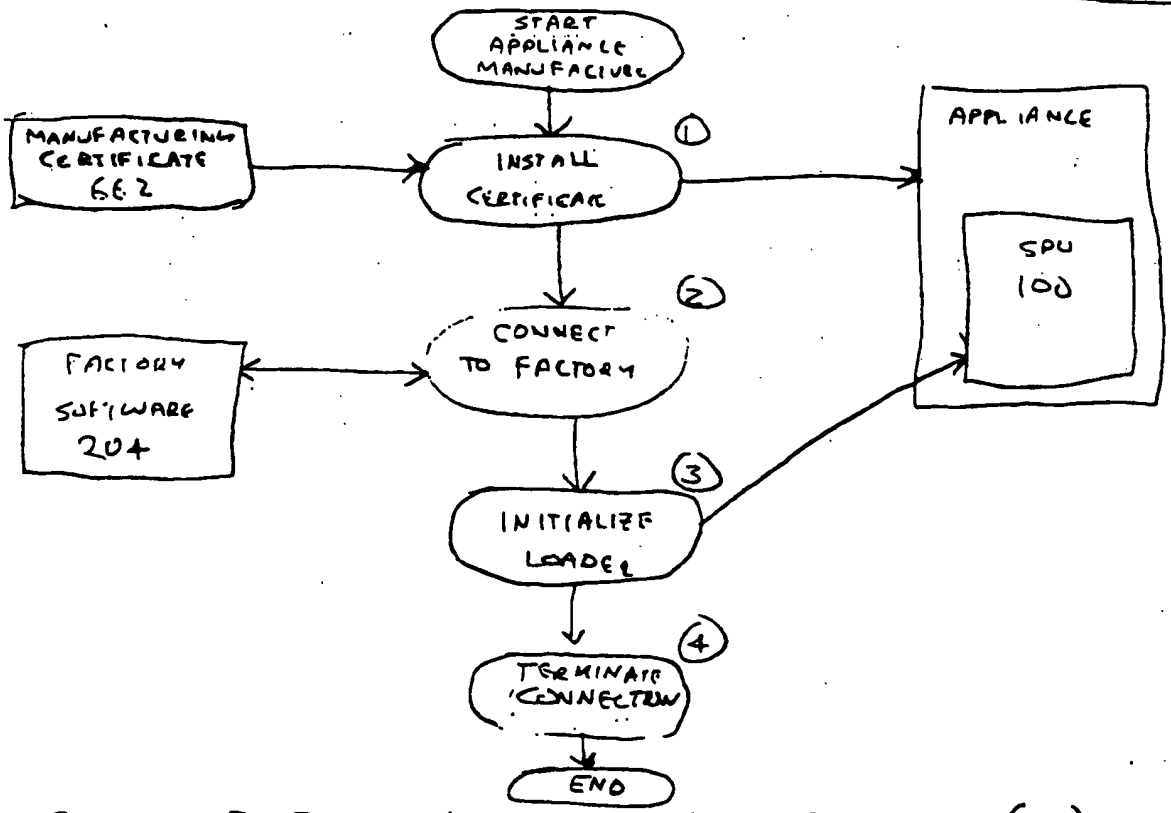


FIGURE 18-B – ALTERNATIVE LOAD PROCESS (2)